

eRed Folder: [First Hit](#)[Previous Doc](#)[Next Doc](#)[Go to Doc#](#)

LZ: Entry 97 of 102

File: JPAB

Nov 1, 1996

PUB-NO: JP408287202A

DOCUMENT-IDENTIFIER: JP 08287202 A

TITLE: DEVICE AND METHOD FOR CERTIFYING IC CARD

PUBN-DATE: November 1, 1996

INVENTOR-INFORMATION:

NAME

COUNTRY

TAWAKITA, TATSUJIRO

ASSIGNEE-INFORMATION:

NAME

COUNTRY

NIPPON TELEGR & TELEPH CORP

APPL-NO: JP07110018

APPL-DATE: April 11, 1995

INT-CL (IPC): G06K 17/00; G06F 15/00

ABSTRACT:

PURPOSE: To obtain the device which is higher in the safety of certification of an IC card than before even if a ciphering function stored on the IC card and at the center of a service provider is stolen by a person who tries to forge certification by controlling the bit length of a random number sent from the center side to the IC card at random.

CONSTITUTION: The center 20 is accessed from the IC card 10. In response, an instruction for reading an ID code is sent out of the center 20 to the IC card 10, which reads its ID code out of an ID code storage memory 13 and sends it out to the center 20. The center 20 once receiving the ID code reads the ciphering key Kn corresponding to the ID code out of an ID and K corresponded memory 23, sends a variable-length random number Xn having random bit length out of a variable-length random number generating means 24 to the IC card 10, and also sends an instruction for writing this variable-length random number Xn to the IC card 10.

COPYRIGHT: (C)1996, JPO

[Previous Doc](#)[Next Doc](#)[Go to Doc#](#)